UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

DICKY WARREN and CARL JUNG, individually and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

FREESTYLE SOFTWARE, INC.,

Defendant.

Case No. 2:22-cv-05533-KM-MAH

FIRST AMENDED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Dicky Warren and Carl Jung ("Plaintiffs"), on behalf of themselves and all others similarly situated, allege the following Class Action Complaint (the "Action") against Defendant Freestyle Software, Inc. ("Defendant" or "Freestyle") upon personal knowledge as to themselves and their own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. Plaintiffs bring this Action on behalf of themselves and all other similarly situated victims of a data breach ("Class Members") in which criminal actors infected Defendant's network with malware and accessed and exfiltrated the data of consumers who interacted with the websites of Defendant's clients for seventeen months before they were detected, from September 18, 2020 through February 3, 2022 (the "Data Breach").

2. Plaintiffs and Class Members were consumers who visited and made purchases on Sturm, Ruger & Company, Inc.'s (hereinafter, "Sturm") website, called "ShopRuger," as well as other retail websites hosted by Defendant and who had their personally identifiable information ("PII") and payment card data ("PCD") compromised, including full names, shipping addresses, email addresses, payment card numbers, expiration dates, security codes, billing addresses, gift certificate numbers, and descriptions of the products purchased on the websites (hereinafter, the "Data Breach"). Not only is this information private, but it is highly sensitive – especially when considering that the purchases by these two particular Plaintiffs were made from a major firearm manufacturer's retail website and not only was there PII and PCD stolen but their home addresses and the nature of their purchases, i.e., firearms and firearm accessories, were disclosed to criminals as well.

3. Defendant has not disclosed any details of the Data Breach to Plaintiffs and Class Members. Instead, Defendant noticed its clients and divulged few details that would allow them to properly inform Plaintiffs and the Class of the Data Breach.

4. On or about August 18, 2022, Sturm began sending letters, titled Notice of Freestyle Solutions[1] Data Breach (the "Notice"), to victims of the Data Breach, including Plaintiffs. According to Sturm, the Data Breach occurred when malware was placed on Defendant's server which hosted the ShopRuger website on or about September 18, 2020. Incredibly, Defendant allowed the malware to exfiltrate non-public data that consumers entered into the ShopRuger website, and other websites it hosted, for nearly seventeen months, from September 18, 2020 through February 3, 2022. Defendant then compounded the harm to Plaintiffs and Class Members by refusing to contact the victims itself, despite purportedly "coordinating with payment card companies in an effort to protect affected cardholders." Instead, six months after it removed the malware from its system, Defendant noticed Sturm and other affected websites of the Data Breach on August 2, 2022. Defendant was apparently unwilling or unable to provide detailed information about the Data Breach According to the Notice, Sturm "had several communications with Freestyle regarding its data breach to assist in [its] review of the matter, but ha[s] been unable to obtain more detailed information." Sturm in turn noticed its own customers sixteen days after Defendant finally disclosed the Data Breach. Defendant's refusal to timely notice Sturm, other affected websites, or Plaintiffs and Class Members, meant that two years had passed from the date of the initial breach before Defendant disclosed the Data Breach.

5. Defendant has not offered any sort of compensation or redress for victims of the Data Breach. Sturm itself has offered its customers identity theft protection services. Defendant

[1] Freestyle Solutions, Inc. was acquired by Vela Software in 2018 and renamed Freestyle Software, Inc. *See* https://velasoftwaregroup.com/vela-software-acquires-freestyle-solutions/

has not offered anything to the victims of this data breach, not even the courtesy of informing Plaintiffs and Class Members themselves.

6. Sturm states in their Notice letter pertaining to Defendant: "this malware was also identified on Freestyle servers hosting of its customers' stores and is not unique to ShopRuger." And, because Defendant has not been forthcoming by informing consumers themselves, by taking an extensive amount of time to respond, and by failing to monitor for malware in the first place, it is conceivable that many other websites who collect similar information from consumers were similarly affected – but those victims are completely unaware because of Defendant's refusal to publicly disclose the Data Breach or offer any compensation or identity monitoring services.

7. Plaintiffs and the proposed Class have suffered injuries as a direct result of the Data Breach include, *inter alia*:

a. Unauthorized charges on their payment card accounts;

b. Theft of their personal and financial information;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. Loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the

actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

f. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and PCD being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class Members' information on the Internet black market and/or dark web;

g. Damages to and diminution in value of their personal and financial information; and,

h. Continued risk to their personal information and PCD, which remains in the possession of Defendant and is subject to further breaches so long as Defendant continues to fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data in its possession.

8. The type of harm suffered by Plaintiffs and the Class is a direct and foreseeable consequence of Defendant's failure to properly secure the sensitive consumer information that it collected and maintained for its own pecuniary benefit as more fully described below.

II. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class,

and at least one member of the class is a citizen of a state different from Defendant, thus establishing the minimal diversity requirement of 28 U.S.C.§ 1332(d).

10. This Court has personal jurisdiction over Defendant because it is incorporated in New Jersey and its corporate headquarters is in Parsippany, New Jersey.

11. Venue is proper in this Court under 28 U.S.C.§ 1391 because a substantial part of the alleged wrongful conduct and events giving rise to the claims occurred in this District and because Defendant conducts significant business in this District.

III. PARTIES

Plaintiff Dicky Warren

12. Plaintiff Dicky Warren is a natural person and a Tennessee resident. Plaintiff Warren made purchases on a Freestyle Software, Inc.-hosted website, ShopRuger, and had his PII and PCD compromised in the Data Breach. Plaintiff Warren received a copy of the Notice described herein and is a Data Breach victim.

Plaintiff Carl Jung

13. Plaintiff Carl Jung is a natural person and a Missouri resident. Plaintiff Jung made purchases on a Freestyle Software, Inc-hosted website, ShopRuger, and had his PII and PCD compromised in the Data Breach. Plaintiff Jung received a copy of the Notice described herein and is a Data Breach victim.

Defendant Freestyle Software, Inc.

14. Defendant Freestyle Software, Inc., a Delaware corporation with its principal place of business in New Jersey, is a software company that provides website hosting and eCommerce solutions to online businesses seeking to sell goods and services directly to consumers.

IV. FACTUAL ALLEGATIONS

Defendant's Business

15. Defendant is a software company that works in the eCommerce sector. The software that Defendant provides allows eCommerce websites to sell goods and services to consumers, like Plaintiffs and members of the Class.[2]

16. Defendant's business would not be possible without the collection and aggregation of consumer data for eCommerce storefronts, like ShopRuger on which it relies to process transactions. In the course of this business, Defendant collects, at a minimum, the PII and PCD that were compromised in the Data Breach as alleged herein. Defendant, as a sophisticated software and website hosting provider, understands the importance of maintaining PII and PCD as private and confidential. Defendant's own terms of use prohibits "violating the privacy rights of others," and "the collection of information about individuals without their knowledge or consent."[3] Despite this, Defendant failed to implement adequate data security measures, to prevent or Detect the Data Breach, and to timely and adequately notice Plaintiffs and Class Members that their most sensitive information had been stolen by criminals.

The Data Breach

17. Sturm's Notice letter contains a number of highly concerning details – including the fact that Sturm was the party to notify consumers as opposed to the Defendant who allowed the Data Breach to occur and failed to detect it for nearly seventeen months.

18. Sturm's Notice letter indicates that cybercriminals implanted malware, malicious code, onto Defendant's server which allowed the cybercriminals to capture Plaintiffs' and Class Members' PII and PCD at a data entry point prior to encryption by Defendant. The Notice letter

[2] https://www.freestylesolutions.com/our-software
[3] https://www.freestylesolutions.com/company/terms-and-conditions/

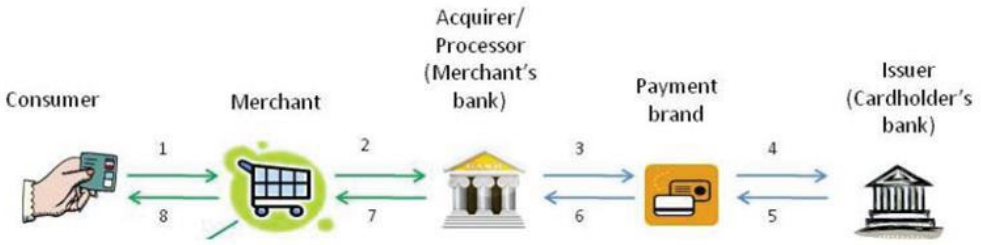
also states that the malware existed on Defendant's server from September 18, 2020 through February 3, 2022, but neither the Notice letter nor Defendant disclosed when they detected the malware and/or Data Breach. Defendant then compounded the issue by refusing to warn Plaintiffs and Class Members and forcing Sturm, and the owners of other affected websites, to disseminate Data Breach notifications based on the limited information provided to them by Defendant on August 2, 2022, six and a half months after the malware had been removed from the Defendant's servers.

19. As stated above, Sturm states in the Notice letter, "this malware was also identified on Freestyle servers hosting of its customers' stores and is not unique to ShopRuger." Defendant has not been forthcoming and has concealed the Data Breach by failing to directly, timely, and adequately inform victims of its lax data security practices. As a result, it is conceivable that many other websites who collect similar information from consumers were similarly affected – but those victims are completely unaware because of Defendant's material omissions and concealment of the Data Breach.

Payment Card Data Breaches

20. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to an e-commerce retailer (through an e-commerce website, like the one ShopRuger presents to consumers) to pay for merchandise. The card is then "swiped" and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (i.e., the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (i.e., cardholder's bank). The issuer then

notifies the payment card company of its decision to authorize or reject the transaction. The below graphic illustrates the process:[4]



1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

21. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

22. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment

[4] Source: "Payments 101: Credit and Debit Card Payments," a white paper by First Data, at: https://www.firstdata.com/downloads/thought-leadership/payments101wp.pdf

it is "swiped," hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the cardholder's personal information stored in the retailer's computers.

The Data Breach was Foreseeable

23. Defendant had obligations created by statute, industry standards, and common law to Plaintiffs and Class Members to keep their PII and PCD confidential and to protect it from unauthorized access and disclosure.

24. Plaintiffs and Class Members provided their PII and PCD to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. Defendant's data security obligations were particularly important given the substantial increase in malware attacks and/or data breaches in industry leaders preceding the date of the breach.

26. Data breaches have become extremely widespread. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[5]

27. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals..

---

[5] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

28. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

29. PII and PCD is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners.

30. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including, upon information and good faith belief, Defendant.

Defendant Failed to Follow FTC Guidelines

31. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

32. According to the FTC, the need for data security should be factored into all business decision-making.

33. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

34. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

35. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

36. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

37. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

38. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

39. Defendant failed to properly implement basic data security practices.

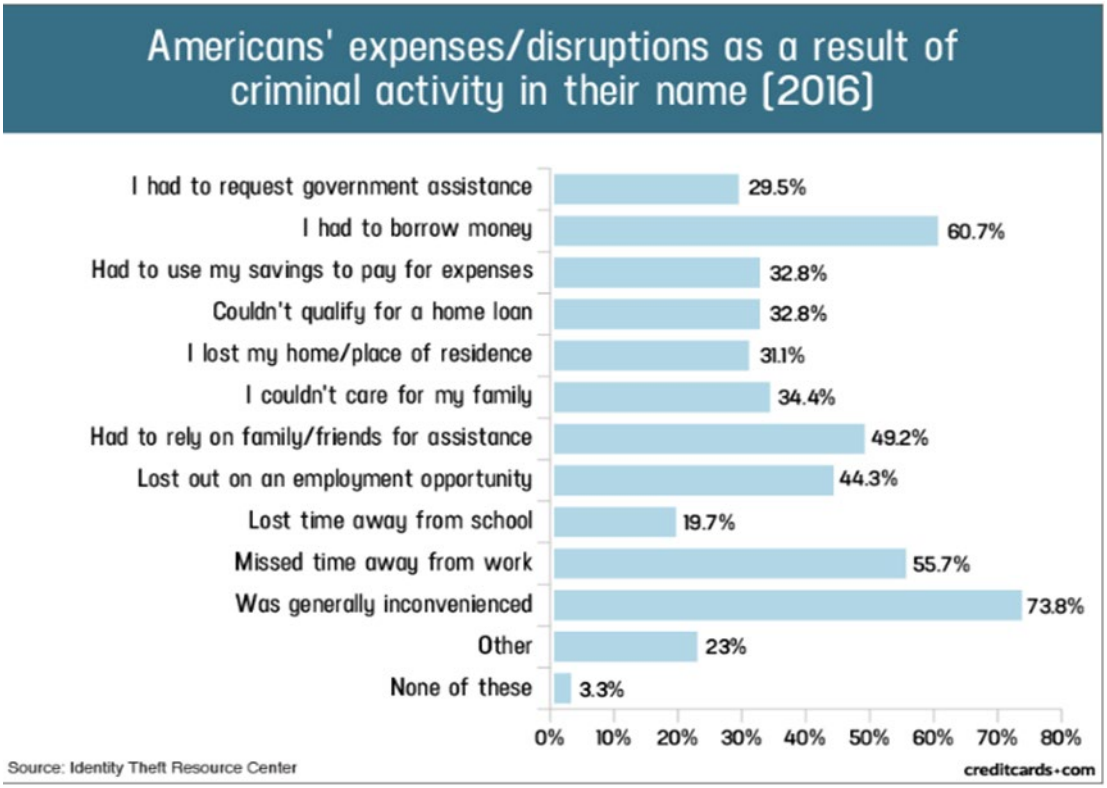
40. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

41. Defendant was at all times fully aware of its obligation to protect the PII and PHI of the patients for whom it stored PII and PHI. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Harm to Consumers and the Value of Personally Identifiable Information

42. The financial fraud suffered by Plaintiffs and other customers demonstrates that Defendant chose not to invest in the technology to encrypt payment card data (PCD) at the point-of-sale to make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or failed to provide sufficient control over employee credentials and access to computer systems to prevent a security breach and/or theft of PCD.

43. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal information:[6]



[6] Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited October 27, 2020).

Plaintiffs and the Class have experienced or most certainly will experience one or more of these harms as a result of the data breach.

44. What's more, theft of PII is also gravely serious. PII is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

45. Once a victim of a data breach a consumer will face harm for years into the future. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

46. PII and financial information, like PCD, are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

47. There is a strong probability that entire batches of stolen information have been dumped on dark web hosted black markets or are yet to be dumped on the black market, meaning that Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

48. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

---

[7] "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" by GAO, June 2007, at: https://www.gao.gov/assets/270/262904.html

credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[9]

49. As a growing number of federal courts have begun to recognize the Loss of Value of PII as a viable damages theory, the sale of PII from data breaches, as in the Data Breach alleged herein, is particularly harmful to data breach victims – especially when it takes place on the dark web.

50. Plaintiffs and Class Members' PII is a valuable commodity, a market exists for Plaintiffs and Class Members' PII (which is why the Data Breach was perpetrated in the first place), and Plaintiffs and Class Members' PII is being likely being sold by hackers on the dark web (as that is the *modus operandi* of data thieves) – as a result, Plaintiffs and Class Members have lost the value of their PII, which is sufficient to plausibly allege injury arising from a data breach.

51. Indeed, federal courts have recently held that, in the data breach context, where the asserted theory of injury is substantial risk of identity theft or fraud, as here, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms.

---

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

[9] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/

52. Plaintiffs and Class Members have or will suffer actual injury as a direct result of Defendant's Data Breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Resetting automatic billing instructions; and

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

53. Plaintiffs and Class Members have been damaged by the compromise of their PII and PCD in the Data Breach.

54. Additionally, Plaintiffs have suffered actual harm in the form of identity theft and/or fraudulent purchase(s) made or attempted on their payment cards using the PII and PCD stolen in the Data Breach as alleged herein.

55. Plaintiffs' PII and PCD was compromised as a direct and proximate result of the Data Breach.

56. As a direct and proximate result of the Data Breach, Plaintiffs' PII and PCD was "skimmed" and exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the identity theft and fraud perpetrated against Plaintiffs as described herein.

57. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered actual identity theft and fraud.

58. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff now has to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

59. Moreover, Plaintiffs and the Class have an interest in ensuring that their information, which remains in the possession of Defendant is protected from further breaches by the implementation of security measures and safeguards.

60. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII and PCD as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

61. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

62. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial records for misuse.

63. Plaintiffs and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including their PII and PCD;

b. Improper disclosure of their personal information and their PII and PCD;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by customers' PII and PCD being placed in the hands of criminals and having been already misused via the sale of such information on the Internet black market;

d. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' PII and PCD for which there is a well-established and quantifiable national and international market; and

h. The loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

64. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their PII and PCD may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

65. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

66. Defendant's substantial delay in providing notice of the Data Breach and continued operation of the compromised e-commerce websites even after discovery of the unauthorized access infecting those sites, deprived Plaintiffs and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class Members was elevated and has been driven even higher.

Plaintiff's Experience

a.) Plaintiff Dicky Warren

67. During the relevant period, Plaintiff Warren made a purchase from the ShopRuger website, which was hosted on Defendant's servers.

68. Plaintiff Warren used one of his debit/credit cards to make this purchase.

69. Subsequent to making this purchase, Plaintiff Warren received a letter dated August 18, 2022, from Sturm, informing Plaintiff Warren that he was the victim of Defendant's Data Breach.

70. The Notice letter informed Plaintiff Warren that malware was placed on the Defendant's servers and that the malware, installed by cybercriminals, allowed those

cybercriminals to gain access to his PII and PCD which he used to make his purchase through the Defendant's servers.

71. Plaintiff Warren's PII and PCD was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the PII and PCD.

72. Plaintiff Warren typically takes measures to protect his PII and PCD and is very careful about sharing his PII and PCD.

73. Plaintiff Warren stores any documents containing his PII and PCD in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

74. As a result of the Data Breach, Plaintiff Warren has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

75. As a result of the Data Breach, Plaintiff Warren made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice letter.

76. Plaintiff Warren also suffered actual injury in the form of damages to and diminution in the value of his PII — a form of intangible property that he entrusted to Defendant for the purpose of processing transactions, which was compromised in and as a result of the Data Breach.

77. Plaintiff Warren suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

78. Plaintiff Warren has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PCD,

particularly his sensitive purchases in combination with his home address, being placed in the hands of criminals.

79. Defendant obtained and continues to maintain Plaintiff Warren's PII and PCD and has a continuing legal duty and obligation to protect that PII and PCD from unauthorized access and disclosure. Defendant required the PII and PCD from Plaintiff Warren when he made purchases from Sturm's website. Plaintiff Warren, however, would not have entrusted his PII and PCD to Defendant had he known that it would fail to maintain adequate data security. Plaintiff Warren's PII and PCD was compromised and disclosed as a result of the Data Breach.

80. As a result of the Data Breach, Plaintiff Warren anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Warren is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

b.) Plaintiff Carl Jung

81. During the relevant period, Plaintiff Jung made a purchase from the ShopRuger, which was hosted on the Defendant's servers.

82. Plaintiff Jung used one of his debit/credit cards to make this purchase.

83. Subsequent to making this purchase, Plaintiff Jung received a letter dated August 18, 2022, from Sturm, informing Plaintiff Jung that he was the victim of Defendant's Data Breach.

84. The Notice letter informed Plaintiff Jung that malware was placed on Defendant's servers and that the malware, installed by cybercriminals, allowed those cybercriminals to gain access to his PII and PCD which he used to make his purchase through the Defendant's servers.

85. Plaintiff Jung's PII and PCD was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the PII and PCD.

86. Plaintiff Jung typically takes measures to protect his PII and PCD and is very careful about sharing his PII and PCD.

87. Plaintiff Jung stores any documents containing his PII and PCD in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

88. As a result of the Data Breach, Plaintiff Jung has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

89. As a result of the Data Breach, Plaintiff Jung made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice letter.

90. Plaintiff Jung also suffered actual injury in the form of damages to and diminution in the value of his PII — a form of intangible property that he entrusted to Defendant for the purpose of processing transactions, which was compromised in and as a result of the Data Breach.

91. Plaintiff Jung suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

92. Plaintiff Jung has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PCD, particularly his sensitive purchases in combination with his home address, being placed in the hands of criminals.

93. Defendant obtained and continues to maintain Plaintiff Jung's PII and PCD and has a continuing legal duty and obligation to protect that PII and PCD from unauthorized access and

disclosure. Defendant required the PII and PCD from Plaintiff Jung when he made purchases from Sturm's website. Plaintiff Jung, however, would not have entrusted his PII and PCD to Defendant had he known that it would fail to maintain adequate data security. Plaintiff Jung's PII and PCD was compromised and disclosed as a result of the Data Breach.

94. As a result of the Data Breach, Plaintiff Jung anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Jung is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

95. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

96. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> Nationwide Class:
>
> All residents of the United States whose PII and/or PCD was compromised as a result of the Data Breach of Defendant's systems from approximately September 18, 2020 through February 3, 2022.

97. Excluded from the above Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

98. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

99. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of at least thousands customers of websites who used the Defendant's eCommerce or website hosting services.

100. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant had a legal duty to adequately protect Plaintiffs' and Class Members' PII and PCD;

c. Whether Defendant breached its legal duty by failing to adequately protect Plaintiffs' and Class Members' PII and PCD;

d. Whether Defendant had a legal duty to provide timely and accurate notice of the data breach to Plaintiffs and Class Members;

e. Whether Defendant breached its duty to provide timely and accurate notice of the data breach to Plaintiffs and Class Members;

f. Whether and when Defendant knew or should have known that Plaintiffs and Class Members' PII and PCD stored on its computer systems was vulnerable to attack;

g. Whether Plaintiffs and Class Members are entitled to recover actual damages and/or statutory damages; and

h. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

101. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII and PCD, like that of every other Class Member, were compromised in the Data Breach.

102. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data breach class actions.

103. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs' and Class Members, in that all the Plaintiffs' and Class Members' PII and PCD was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

104. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management

difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

105. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Defendant has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

106. Finally, all members of the purposed Class are readily ascertainable. Defendant has access to addresses and other contact information for members of the Class, which can be used to identify Class Members.

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE

107. Plaintiffs reallege and restate all of the paragraphs above and below as if fully incorporated herein.

108. Plaintiffs bring this count on behalf of themselves and the Class.

109. Defendant required Plaintiffs and the Class Members to submit non-public personal information in order to obtain consumer goods through the websites for which Defendant partners provides eCommerce and hosting services.

110. The Class members are individuals who provided certain PII and PCD to Defendant including the PII and PCD described above.

111. Defendant had full knowledge of the sensitivity of the PII and PCD with which it was entrusted and the types of harm that Class members could and would suffer if the information were wrongfully disclosed.

112. Defendant had a duty to each Class member to exercise reasonable care in holding, safeguarding and protecting that information.

113. Plaintiffs and the Class members were the foreseeable victims of any inadequate safety and security practices.

114. The Class members had no ability to protect their data in Defendant's possession.

115. By collecting and storing this data in its computer property, and by using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and the Class members' PII and PCD held in it — to prevent disclosure of the information and to safeguard the information from theft.

116. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

117. Defendant owed a duty of care to safeguard the PII and PCD of Plaintiffs and Class members in its custody. This duty of care arises because Defendant knew of a foreseeable risk to the data security systems it used. Defendant knew of this foreseeable risk because of the explosion of ransomware and data breach incidents involving online retailers as detailed above. Despite its knowledge of this foreseeable risk, Defendant failed to implement reasonable security measures.

118. Defendant owed a duty of care to Plaintiffs and the Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected Private Information

119. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

120. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PCD.

121. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Class members' PII and PCD.

122. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures to safeguard Class members' PII and PCD;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class members' PII and PCD;

e. Failing to detect in a timely manner that Class members' Private Information had been compromised;

f. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages and

g. Failing to have mitigation and back-up plans in place in the event of a cyber- attack and data breach.

123. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII and PCD would result in injury to Plaintiffs and Class members.

124. Further, the breach of security was reasonably foreseeable given the known high frequency of hacking incidents, cyberattacks, and data breaches in the online commerce industry.

125. It was therefore foreseeable that the failure to adequately safeguard Class members' PII and PCD would result in one or more types of injuries to Class members.

126. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Breach.

127. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) provide adequate credit monitoring to all Class members.

COUNT II

NEGLIGENCE PER SE

128. Plaintiffs reallege and restate all of the paragraphs above and below as if fully incorporated herein.

129. Plaintiffs bring this count on behalf of themselves and the Class.

130. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII and PCD.

131. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

132. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PCD it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiffs and the Class.

133. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

134. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

135. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

136. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Plaintiffs' and Class Members' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members.

137. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

138. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

139. As a direct and proximate result of Defendant's negligence per se, Plaintiffs are now at an increased risk of identity theft or fraud.

140. As a direct and proximate result of Defendant's negligence per se, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT III

VIOLATION OF NEW JERSEY CONSUMER FRAUD ACT

N.J.S.A. § 56:8-2, *et seq*.

141. Plaintiffs reallege and restate all of the paragraphs above and below as if fully incorporated herein.

142. Plaintiffs bring this count on behalf of themselves and the Class.

143. The New Jersey Consumer Fraud Act ("New Jersey CFA") makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression

or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby." N.J.S.A. § 56:8-2.

144. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

a. failing to maintain adequate computer systems and data security practices to safeguard PII;

b. failing to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. continuing to gather and store PII, and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the data breach;

d. continuing to gather and store PII, and other personal information after Defendant knew or should have known of the Data Breach and before Defendant allegedly remediated the data security incident;

e. continuing to store and maintain the PII of former customers when Defendant had no legitimate business need to do so; and

f. delaying in notifying the Plaintiffs and Class Members of the Data Breach, and the full scope of the Data Breach.

145. These unfair acts and practices violated duties imposed by laws, including, but not limited to the FTCA, the New Jersey Deceptive and Unfair Trade Practices Act, and the New Jersey CFA.

146. Defendant's delay in notifying the victims of the Data Breach also violates provisions of the New Jersey Consumer Security Breach Disclosure Act, which required Defendant, once it knew or had reason to know of a data security breach involving personal information, to provide prompt and direct notice of such breach to any affected, indicating another deceptive act and practice.

147. The foregoing deceptive acts and practices emanated from New Jersey and were directed at consumers/purchasers in New Jersey and in each state where Defendant did business.

148. Defendant, Plaintiffs, and Class Members are "persons" within the meaning of N.J.S.A. § 56:8-1(d).

149. Defendant engaged in "sales" of "merchandise" within the meaning of N.J.S.A. § 56:8-1(c), (d).

150. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the services provided, specifically as to the safety and security of PII and PCD, and other personal and private information, to induce consumers to purchase the same.

151. DEFENDANT's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Class Action Complaint are material in that they relate to matters which reasonable persons, including Plaintiffs and Members of the Class, would attach importance to in making their purchasing decisions or conducting themselves regarding their purchases using services provided by Defendant.

152. Plaintiffs and Class Members are consumers who made payments to Defendant's clients that were primarily for personal, family, or household purposes.

153. Defendant engaged in the conduct alleged in this Complaint, entering transactions intended to result, and which did result, in the furnishing of services to consumers, including Plaintiffs and Class Members. Defendant's acts, practices, and omissions were done in the course of Defendant's business of marketing, offering to sell, and furnishing services from the State of New Jersey. As a direct and proximate result of Defendant's multiple, separate violations of N.J.S.A. § 56:8-2, Plaintiffs and the Class Members suffered damages including, but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (g) the diminished value of Defendant's services they received.

154. Also as a direct result of Defendant's violation of the New Jersey CFA, Plaintiff and the Class are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members. Plaintiffs and Class Members were injured because: (a) they would not have paid using Defendant's services had they known the true

nature and character of Defendant's data security practices; (b) would not have entrusted their PII or PCD to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and (c) would not have entrusted their PII or PCD to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

155. As a result, Plaintiffs and the Class Members have been damaged in an amount to be proven at trial.

156. On behalf of themselves and other members of the Class, Plaintiffs and Class Members are entitled to recover legal and/or equitable relief, including an order enjoining Defendant's unlawful conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J.S.A. § 56:8-19, and any other just and appropriate relief.

COUNT IV

UNJUST ENRICHMENT

157. Plaintiffs reallege and restate all of the paragraphs above and below as if fully incorporated herein.

158. Plaintiffs bring this count on behalf of themselves and the Class.

159. This count is pleaded in the alternative to Count II above.

160. Plaintiffs and members of the Class conferred a monetary benefit on Defendant in the form of payments using Defendant's services and the provision of their PII and PCD, without which Defendant would be unable to carry out its regular business. Specifically, they made purchases from websites that Defendant partners with to provide eCommerce software and hosting solutions and provided Defendant with their PII and PCD. Plaintiffs would not have made these

purchases, or would have paid less, had they known that Defendant did not provide adequate protection of their PII and PCD.

161. By providing their PII and PCD to Defendant and/or making payment through Defendant's services, Plaintiffs and members of the Class expected that a portion of Defendant's revenue derived from their use of its services would be used to fund adequate data security to protect their PII and PCD. Instead, Defendant diverted those funds to its own profit and at the expense of Plaintiffs and Class members who are now left to deal with the consequences of the Data Breach on their own.

162. Defendant knew and appreciated that Plaintiffs and the Class conferred a benefit on it by providing their PII, PCD, and making their payments via its services. Defendant also profited from their use of their PII and PCD and would be unable to engage in its regular business activities without the PII and PCD entrusted to it by Plaintiffs and Class Members.

163. Defendant failed to secure Plaintiffs' and Class Members' PII and PCD, and therefore was unjustly enriched by the purchases made by Plaintiffs' and the Class that they would not have made had they known that Defendant did not keep their PII and PCD secure.

164. Plaintiffs and the Class have no adequate remedy at law and no contract exists that would govern the relationship between Plaintiffs and Class Members and Defendant.

165. Under the circumstances, it would be unjust and inequitable for Defendant to be permitted to retain any of the benefits and profits derived therefrom that Plaintiffs' and Class Members conferred on it.

166. Defendant should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class Members proceeds that it unjustly received from them.

COUNT V

DECLARATORY JUDGMENT

167. Plaintiffs reallege and restate all of the paragraphs above and below as if fully incorporated herein.

168. Plaintiffs bring this count on behalf of themselves and the Class.

169. Defendant was required to provide adequate security for the PII and PCD it collected from the payment card transactions of Plaintiffs and members of the Class.

170. Defendant owes duties of care to Plaintiffs and the members of the Class that require it to adequately secure the PII and PCD it collected for its own pecuniary benefit.

171. Defendant still possesses the PII and PCD of Plaintiffs and the Class Members and Defendant has not indicated that it has implemented enhanced security measures or destroyed the PII of Plaintiffs and Class Members that it collected and retained.

172. Defendant is at a heightened risk of another data breach due to the knowledge acquired by the attackers that can be used to exploit existing vulnerabilities in Defendant's security measures. Defendant is also susceptible to attacks by other groups who are now aware of the fact that Defendant's security was so lax that it allowed malware to exist on its server for nearly seventeen months.

173. Accordingly, Defendant still has not satisfied its legal duties to Plaintiff sand the Class. Due to the fact that Defendant's inadequate data security has become public, the PII and PCD in Defendant's possession is more vulnerable than it was previously.

174. Actual harm has arisen in the wake of Defendant's data breach regarding its duties of care to provide security measures to Plaintiffs and the members of the Class. Further, Plaintiffs

and the members of the Class are at risk of additional or further harm due to the exposure of their PII and PCD and Defendant's failure to address the security failings that lead to such exposure.

175. There is no reason to believe that Defendant's security measures are any more adequate than they were before the breach to meet Defendant's contractual obligations and legal duties, particularly given Defendant's concealment of the Data Breach and failure to adequately notify affected websites and Plaintiffs and Class Members.

176. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its legal obligations to provide adequate security, and (2) that to comply with its legal obligations and protect Plaintiffs and Class Members, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach, and

h. Ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of personal information to third parties, as well as the steps its customers must take to protect themselves.

VII. PRAYER FOR RELIEF

177. **WHEREFORE,** Plaintiffs, on behalf of themselves and the Class, seek the following relief:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class;

b. Judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein.

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. JURY TRIAL DEMAND

178. Plaintiffs demand a trial by jury on all triable issues.

DATED: November 15, 2022

Respectfully submitted,

s/ Victoria Maniatis

Victoria Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (212) 594-5300
Email: **vmaniatis@milberg.com**

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Tel.: 866-252-0878
gklinger@milberg.com

ATTORNEYS FOR PLAINTIFFS

*Pro Hac Vice Forthcoming